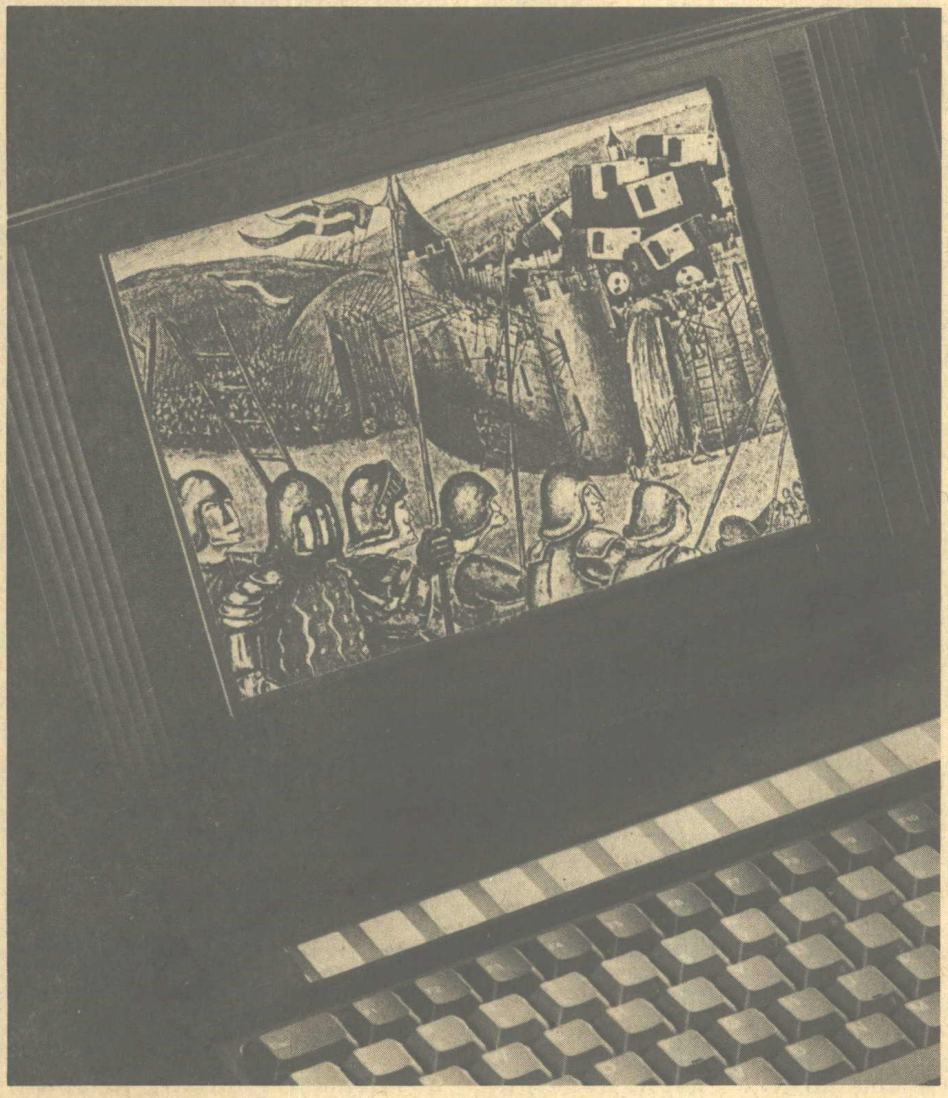
ลิขสิทธิ์ นำชัย

มารักษา ความปลอดภัย ให้ข้อมูลกันเถอะ

สร้างมาตรการการป้องกัน และรักษาความปลอดภัย ของข้อมูลในระบบคอมพิวเตอร์ ของคุณให้เข้มงวดยิ่งขึ้น



ข้อมูลต่าง ๆ ไม่ว่าจะเป็นข้อมูลอะไร ข้อมูลส่วนตัวหรือข้อมูลทางธุรกิจ ข้อมูลแต่ละชุดนั้นมีค่าเฉพาะตัวที่แตกต่างกันไป ข้อมูลบางอย่างอาจมีค่ามากจนไม่สามารถประเมินได้ ในขณะที่ข้อมูลบางชุดนั้นเป็นเพียงขยะที่ทำให้เสียเนื้อที่และเวลาในการจัดเก็บเท่านั้น ดังนั้นการบริหารในการจัดเก็บข้อมูลจึงเป็นเรื่องที่สำคัญมากเรื่องหนึ่งของทุก ๆ คนทุก ๆ หน่วยงาน โดยเฉพาะอย่างยิ่งกับการจัดเก็บและดูแลข้อมูลที่มีความสำคัญ เพราะหากข้อมูลสำคัญหรือเป็นความลับนั้นถูกทำลายหรือถูกเผยแพร่ออกไปย่อมก่อให้เกิดความเสียหายอย่างมาก โดยเฉพาะอย่างยิ่งหากข้อมูลเหล่านั้นตกอยู่กับคู่แข่งหรือฝ่ายตรงข้าม ดังจะเห็นได้ว่าทุกยุคทุกสมัยจะมีการสอดแนมหรือการส่งบรรดาจารชนเข้าไปทำการจารกรรมข้อมูลของหน่วยงานที่เป็นฝ่ายตรงข้ามเสมอ

สำหรับในปัจจุบัน ในยุคที่เรียกกันอย่างเต็มปากว่าโลกานุวัตร ข้อมูลทุกอย่างนั้นได้ถูกบันทึกเก็บไว้ในเครื่องคอมพิวเตอร์ตามความนิยม ตั้งแต่โรงเรียนในประเทศด้อยพัฒนาบางประเทศที่นักเรียนยังยากจนและขาดแคลนอาหารกลางวันอยู่ แต่ผู้บริหารกลับมีนโยบายใช้งบประมาณที่มีซื้อคอมพิวเตอร์

มาใช้ช่วยในการเรียนการสอนเพื่อให้ดูทันสมัย จนกระทั่งถึงหน่วยงานที่เป็นองค์กรใหญ่ระดับโลกของประเทศที่เรียกตัวเองว่าประเทศมหาอำนาจ ดังนั้นการป้องกันหรือการรักษาความปลอดภัยข้อมูลที่อยู่ในระบบคอมพิวเตอร์จึงเป็นเรื่องสำคัญมากในปัจจุบัน โดยเฉพาะอย่างยิ่งกับเครื่องที่เชื่อมกับเครื่องหรือเครือข่ายอื่น

รักษาความปลอดภัยข้อมูลเพื่ออะไร

เป้าหมายในการรักษาความปลอดภัยข้อมูลในระบบคอมพิวเตอร์ไม่ว่าเป็นระบบใดก็ตาม หากสามารถรักษาคุณสมบัติหลักได้ดังนี้ ก็นับได้ว่าการรักษาความปลอดภัยข้อมูลประสบความสำเร็จ

1) รักษาสิ่งต่าง ๆ เป็นความลับ (Security) ให้เป็นความลับอยู่ได้ และข้อมูลเหล่านั้นจะเข้าถึงได้เฉพาะบุคคลที่ได้รับสิทธิเท่านั้น

2) รักษาความปลอดภัยได้ง่าย (Integrity) ข้อมูลต่าง ๆ จะทำการแก้ไขหรือเปลี่ยนแปลงได้เพียงบุคคลที่ได้รับสิทธิเท่านั้น ผู้อื่นจะทำการเปลี่ยนแปลงแก้ไขไม่ได้ ตลอดจนกลไกการดำเนินการทำได้ง่าย

3) รักษาความสมดุล (Availability) ข้อมูลจะต้องเข้าถึงได้เสมอ ภายใต้เงื่อนไขว่า ผู้ใช้นั้นเป็นผู้มีสิทธิ์ในอุปกรณ์และข้อมูลนั้น ๆ

อันตรายใดบ้างที่จะทำลายข้อมูล

ก่อนที่จะรู้เกี่ยวกับหลักการหรือวิธีการป้องกันและรักษาความปลอดภัยข้อมูล มาดูซิว่าบุคคลใดบ้างที่จะก่อให้เกิดความเสียหายกับระบบ ซึ่งบุคคลหรือเหตุการณ์เหล่านี้ผู้ใช้อาจไม่เคยใส่ใจเลยก็ได้

ผู้ใช้งานที่ไม่มีความรู้เพียงพอ

สำหรับเครื่องที่มีการใช้งานร่วมกัน ไม่ว่าจะเป็นเครื่องพีซีธรรมดาหรือเครื่องที่เป็นแบบผู้ใช้หลายคนก็ตาม โอกาสการทำงานร่วมกันแล้วส่งผลกระทบถึงกันนั้นอาจเกิดขึ้นได้ ไม่ว่าจะเป็นการจงใจหรือพลั้งเผลอ เช่น อาจเผลอลบหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญ อันตรายที่เกิดจากบุคคลในกลุ่มนี้ส่วนใหญ่มักเกิดจากการยืมเครื่องหรือรายชื่อและรหัสผ่านกันใช้

พวกสอดรู้สอดเห็น หรืออยากลองวิชา (Hacker)

บุคคลกลุ่มนี้ส่วนใหญ่จะเป็นนักคอมพิวเตอร์ที่มีความสามารถพิเศษชอบความท้าทาย โดยเฉพาะอย่างยิ่งต้องการที่จะชอนไชเจาะระบบที่มีข้อมูลสำคัญที่มีการเตรียมการป้องกันรักษาความปลอดภัยไว้แล้วแต่อาจมีช่องโหว่อยู่บ้าง โดยส่วนใหญ่แล้วบุคคลในกลุ่มนี้จะแบ่งเป็นสองฝ่ายคือ ฝ่ายธรรมะและอธรรม โดยหากเป็นแฮกเกอร์ที่อยู่ฝ่ายธรรมะเมื่อเจาะเข้าระบบและพบข้อบกพร่องหรือช่องโหว่ของระบบแล้ว ก็เพียงแค่ประกาศและแจ้งจุดอ่อนของระบบแก่ผู้ดูแลระบบทราบเท่านั้น แต่สำหรับแฮกเกอร์อีกกลุ่มนั้นซึ่งมีอยู่เป็นจำนวนไม่น้อยที่พบช่องโหว่และจะตามชอนไชไปทั่วระบบแล้วถือโอกาสทำลายหรือเปลี่ยนแปลงข้อมูลสำคัญ บุคคลในกลุ่มนี้เป็นที่หนักใจของบรรดาผู้ดูแลระบบทั้งหลายที่จะทำการป้องกัน

พวกสอดแนม ล้วงความลับเกี่ยวกับข้อมูล

พวกนี้จะมีเจตนาร้าย โดยจะล้วงความลับเกี่ยวกับข้อมูลมากกว่าการทำลายข้อมูล โดยเฉพาะอย่างยิ่งข้อมูลทางธุรกิจ ซึ่งถือว่าเป็นความลับที่มีความสำคัญต่อบริษัทอย่างมาก

ผู้ใช้ที่ต้องการทำลายเอง

มีจำนวนไม่น้อยที่ปัญหาเกี่ยวกับการรักษาความปลอดภัยข้อมูลเกิดจากการที่ผู้ใช้ภายในระบบเองอาจไม่พอใจอะไรบางประการเลยหาทางระบายออกหรือแก้แค้น โดยการทำลายระบบการรักษาความปลอดภัยของข้อมูลเอง

อุบัติเหตุ

อุบัติเหตุต่าง ๆ ที่เกิดขึ้นตามธรรมชาติและมนุษย์เป็นผู้ก่อ เช่น ไฟไหม้ แผ่นดินไหว หรือเหตุการณ์ใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบ

ระบบรักษาความปลอดภัยต้องเป็นอย่างไร

การออกแบบระบบการรักษาความปลอดภัยข้อมูลเป็นเรื่องที่ยุ่งยากมาก เพราะหากการควบคุมอย่างเข้มงวดจนเกินไป มีข้อจำกัดจุกจิกมากมายจนทำให้การใช้งานเหมือนเป็นเรื่องที่ยุ่งยากวุ่นวาย ผู้ใช้งานจะรู้สึกเกร็งในเวลาที่ใช้งาน เพราะจะทำอะไรต้องระมัดระวังไปหมด คงจะเป็นที่ลำบากใจกันมากทีเดียว ดังนั้นการรักษาความปลอดภัยข้อมูลที่ดีต้องคำนึงถึงหลักการต่าง ๆ มากพอสมควร

1. ระบบรักษาความปลอดภัยต้องง่ายและตรงไปตรงมา และกลไก

รักษาความปลอดภัยต้องใช้ง่าย เพราะถ้าหากยุ่งยากแล้วผู้ใช้ส่วนใหญ่จะละเลยเสีย

2. ในกรณีที่เป็นระบบที่มีการใช้งานร่วมกันหลายคน ผู้ใช้แต่ละคนในระบบควรจะได้รับสิทธิ์น้อยที่สุดเท่าที่พอเพียงในการทำงานเท่านั้น เพื่อป้องกันความเสียหายที่อาจกระทบต่อข้อมูลในส่วนอื่นได้โดยไม่ได้ตั้งใจ

3. ให้ระบบมีการตรวจสอบอย่างรอบคอบในการเข้าถึงหรือการทำงานทุกอย่าง

4. การลงทุนในมาตรการรักษาความปลอดภัยข้อมูลนั้นอยู่ที่ความเหมาะสมกับความสำคัญของข้อมูล มิฉะนั้นจะเป็นการลงทุนที่เกินตัว ตรงกับสุภาษิตที่ว่าขี่ช้างจับตั๊กแตน

กลยุทธ์ในการเข้าทำลายข้อมูล

กรรมวิธีที่จะใช้ในการเข้าทำลายข้อมูลนั้นมีอยู่หลายวิธี ขึ้นอยู่กับมาตรการการรักษาความปลอดภัยข้อมูลของแต่ละคน แต่ละหน่วยงาน และระดับศักยภาพหรือสถานภาพของผู้ที่จะเข้าทำลายข้อมูล

1) แอบดูรหัสผ่านในขณะพิมพ์ในกรณีที่เป็นบุคคลที่ใกล้ชิดกัน

2) ใช้เครื่องมือจับที่เรียกว่า "โปรโตคอลอนาไลเซอร์" เครื่องวิเคราะห์โปรโตคอลไปดักจับรหัสผ่านในกรณีที่มีช่วงระยะเชื่อมต่อระหว่างตัวเครื่องที่ใช้งานกับส่วนของระบบ อย่างเช่นการใช้งานโดยผ่านโมเด็ม

3) บูตระบบใหม่ ระบบปฏิบัติการบางตัว เช่น ในยูนิกซ์บางรุ่นจะเริ่มต้นระบบใหม่ด้วยการทำงานอยู่ในโหมดของผู้ใช้งานคนเดียวหรือผู้ดูแลระบบก่อน ซึ่งหากเป็นเช่นนี้ถ้าผู้ทำลายระบบสามารถเริ่มต้นระบบใหม่ได้ก็เท่ากับว่าการทำลายระบบสำเร็จไปมากกว่าครึ่งแล้ว แต่ส่วนใหญ่ระบบยูนิกซ์ในปัจจุบันมักจะให้เริ่มต้นระบบโดยเข้าสู่โหมดผู้ใช้หลายคนเลย ถึงแม้ว่าขณะเริ่มจะเป็นช่วงที่เป็นโหมดผู้ใช้งานคนเดียวก่อนก็ตาม ระบบจะสอบถามถึงรหัสผ่านของผู้ดูแลระบบก่อน หากรหัสผ่านไม่ถูกต้องภายในเวลาหรือจำนวนครั้งที่กำหนด ระบบจะเข้าสู่โหมดผู้ใช้งานหลายคนแทน

4) รันโปรแกรมทิ้งไว้โดยโปรแกรมนั้นอาจเป็นโปรแกรมที่มีการสร้างจอภาพหรือจำลองสถานการณ์ให้ผู้ใช้ป้อนรหัสผ่าน โดยโปรแกรมจะรอให้ผู้ใช้ที่ไม่ระวังพิมพ์ชื่อผู้ใช้และรหัสผ่านเข้าสู่โปรแกรมแล้วทำการส่งชื่อผู้ใช้และรหัสผ่านไปยังตนเอง หรือโปรแกรมเล็ก ๆ ที่เขียนขึ้นมาในลักษณะพิเศษเพื่อให้สามารถเพิ่มสิทธิ์การจัดการของตนเองให้เพิ่มขึ้นจากเดิม หรือโปรแกรมที่มีการใช้พจนานุกรมเป็นส่วนร่วมในการแกะรหัสผ่านของผู้ใช้งานในระบบ

จะควบคุมและดูแลได้อย่างไรบ้าง

การดูแลรักษาความปลอดภัยข้อมูลคอมพิวเตอร์นั้นต้องทำครอบคลุมทั้งทางด้านฟิสิคัล (Physical) และทางลอจิกคัล (Logical) มาตรการสำหรับการรักษาความปลอดภัยของข้อมูลนี้มิได้หมายความว่าเพียงแค่ป้องกันการจารกรรมหรือการขโมยข้อมูลจากบุคคลที่ไม่พึงปรารถนาเท่านั้น แต่ยังรวมไปถึงการป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลด้วย

Physical Security

เป็นการป้องกันโดยกายภาพ โดยป้องกันไม่ให้ผู้ที่จะมาทำลายหรือเหตุการณ์ต่าง ๆ ที่จะก่อให้เกิดความเสียหายของข้อมูลเกิดขึ้นได้ อาจจะทำได้เป็น

1) ระวังบุคคลแปลกปลอมเข้ามาใช้งานระบบ โดยอาจจะมีการจัดเวรยามดูแลหรือจัดสถานที่การทำงานที่เหมาะสม

2) มีการล็อกอุปกรณ์ที่สำคัญที่ใช้งานในระบบ

3) หมั่นตรวจสอบข้อมูลและสำรองข้อมูลสำคัญไว้ในอุปกรณ์ภายนอก เช่น เทป ดิสก์ แล้วทำการลบข้อมูลที่สำคัญหรือเป็นข้อมูลลับในระบบออก

4) การจัดสภาวะแวดล้อมของระบบให้เหมาะสม เช่น มีระบบพลังงานสำรอง หรือระบบดับเพลิงไว้ใช้ในยามฉุกเฉิน

Logical Security

เป็นการป้องกันภายในตัวของระบบเอง โดยจะแบ่งได้เป็น 2 ประการหลัก ๆ คือ การตรวจสอบผู้ใช้ และการเข้ารหัสไฟล์

การตรวจสอบผู้ใช้

ในระบบปฏิบัติการส่วนใหญ่หรือแม้แต่ตัวโปรแกรมหลาย ๆ โปรแกรมในปัจจุบันนี้จะมีการตรวจสอบผู้ใช้งานโดยจะถามถึงรายชื่อ (user name) และรหัสผ่าน (password) โดยระบบจะทำการตรวจสอบรหัสผ่านที่ผู้ใช้ป้อนเข้ามากับรหัสผ่านที่อยู่ในฐานข้อมูลของระบบว่าตรงกันหรือไม่ และจะอนุญาตให้ผู้ใช้ทำงานได้ทันทีหลังจากตรวจสอบแล้วพบว่ารหัสผ่านนั้นถูกต้อง รหัสผ่านจึงนับว่าเป็นส่วนสำคัญส่วนหนึ่งที่ใช้ในการรักษาความปลอดภัยของข้อมูล

Input Data	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
p	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
f(p)=(p+3)mod26	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
Output Data	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

ตารางที่ 1

kdfnhu Lqlwldoob, d vhulrxv frpsxwhu-xvhu. Wkh whup qrz uhihuv wr d shuvrq zkr jdlqv xqdxwkrulchg dffhvv wr d frpsxwhu vbvwhp dqg wkhq wulhv wr pdvwhu wkh dssolfdwlrqv dqg vrphwlphv pdnh prglilfdwlrqv. Vrph kdfnhuv hqwhu vbvwhpv mxvw iru ixq, zkloh rwkhuv lqwhqwlrqdoob fdxvh gdpdjh eb hlwkhu frpplwwlqj iudxg, ru ghvwurblqj ydoxdeoh gdwd. Pdqb frxqwulhv wuhdw kdfnhuv dv fulplqdov zkr fdq lqfxu wkh vdph shqdowlhv dv wkrvh lpsrvhg rq euhdn-dqg-hqwhu fulplqdov.

รูปที่ 1 ตัวอย่างจดหมายที่เข้ารหัสด้วยกรรมวิธีของจูเลียส ซีซาร์

ทำอย่างไรกับรหัสผ่านดี

1) เก็บรักษารหัสผ่านเป็นความลับ ไม่ควรบันทึกหรือสำเนารหัสผ่านไว้ ดังนั้นผู้ใช้จำเป็นต้องจำรหัสผ่านให้ได้ มิฉะนั้นแล้วนอกจากผู้อื่นไม่สามารถใช้ข้อมูลได้ ตัวผู้ใช้เองก็ไม่สามารถใช้งานได้ด้วย

2) ให้ตั้งรหัสผ่านที่มีทั้งสระ พยัญชนะ ตัวเลข และสัญลักษณ์พิเศษประสมกันเป็นรูปแบบของกลุ่มตัวอักษรที่ไม่มีความหมาย เพราะบรรดาผู้ใช้ส่วนใหญ่มักจะนำชื่อตนเอง ชื่อแฟน ชื่อดารา ตัวละครในนวนิยาย เบอร์โทรศัพท์ สถานที่สำคัญ สิ่งที่ประทับใจ ซึ่งบุคคลที่รู้จักสามารถคาดเดาได้ง่าย

3) อย่าใช้คำศัพท์ที่มีอยู่ในพจนานุกรมมาตั้งเป็นรหัสผ่าน เพราะบรรดาโปรแกรมที่ใช้ในการถอดรหัสผ่านหลายตัวนั้นใช้กรรมวิธีการตรวจเช็คจากพจนานุกรม ซึ่งโอกาสที่การถอดรหัสหรือการทำนายนั้นถูกต้องเป็นเปอร์เซ็นต์ที่สูง

4) หมั่นเปลี่ยนรหัสผ่านให้บ่อยเท่าที่สามารถกระทำได้ ในระบบปฏิบัติการหลายประเภทเช่นเน็ตแวร์หรือยูนิกซ์ สามารถกำหนดระยะเวลาในการใช้งานหรือระยะเวลาในการเปลี่ยนรหัสผ่านใหม่สำหรับผู้ใช้งานแต่ละคนได้ หรือแม้แต่กำหนดรูปแบบของการตั้งรหัสผ่าน เช่น ต้องมีอักษรตัวเล็กและตัวใหญ่กี่ตัว และรหัสใหม่ต้องต่างจากรหัสเก่าอย่างไร

5) เลือกรหัสผ่านที่สามารถพิมพ์ได้อย่างรวดเร็วและถูกต้อง จำได้ง่าย แต่เดาได้ยาก

6) ไม่แบ่งให้ผู้อื่นใช้งานร่วมด้วย

การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูลเป็นอีกวิธีหนึ่งที่มีการใช้งานกันมากในระบบหลาย ๆ ระบบในแง่ของการป้องกันล่วงรู้เนื้อความภายใน การที่จะเข้าใจข้อมูลภายในแฟ้มที่เข้ารหัสข้อมูลนั้นได้จะต้องรู้ถึงกุญแจหรือกรรมวิธีการเข้ารหัสก่อนแล้วจึงจะสามารถถอดรหัสข้อมูลได้ การเข้ารหัสข้อมูลนี้มีการใช้งานมานานตั้งแต่อดีต อย่างเช่น อัลกอริทึมการเข้ารหัสเนื้อความในจดหมายของ จูเลียส ซีซาร์ (Julius Caesar) ที่ใช้วิธีการเลื่อนตัวอักษรไปอีก 3 ตัว ดังตารางที่ 1 ส่วนรูปที่ 1 นั้นเป็นตัวอย่างของจดหมายที่เข้ารหัสด้วยวิธีการของจูเลียส ซีซาร์ (ลองแกะกันดูนะครับ) ซึ่งต่อมาอัลกอริทึมนี้ก็ได้มีการพัฒนาจนกลายเป็นอัลกอริทึมต่าง ๆ ที่สลับซับซ้อนมากยิ่งขึ้นอีกจำนวนมาก

สรุป

ความปลอดภัยของข้อมูลเป็นสิ่งที่สำคัญและตื่นตัวกันมาก ปัญหาหลักเรื่องนี้ขึ้นอยู่กับผู้ใช้งานเอง เพราะถึงแม้ในระบบจะมีวิธีหรือมาตรการที่ดีเพียงใดก็ตาม หากผู้ใช้งานไม่เห็นความสำคัญและไม่ปฏิบัติตาม การรักษาความปลอดภัยของระบบนั้นก็ล้มเหลว